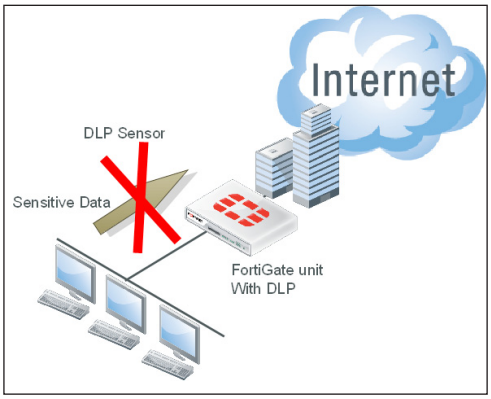
Data Leak Prevention (DLP)

Data Leak Prevention uses digital markers and pattern matching techniques to identify and prevent unauthorized communication of sensitive information outside the network.

Preventing data leaks

Data leaks are an increasingly important issue for organizations worldwide that use and store sensitive data. A data leak can be both embarrassing and costly, regardless of whether it was intentional or not. Data leaks damage confidence and trust in your network's security. Damage of this type can require a major investment of time and resources to undo.

Data Leak Prevention (DLP), also known as Data Loss Prevention, provides a way to prevent data leaks from occurring either intentionally or by accident.



DLP

DLP differs from most security measures because it primarily monitors internal network data rather than focusing on threats from external sources. DLP uses a variety of digital markers and pattern identification techniques to identify documents containing sensitive data and block them from leaving the network.

FortiOS DLP protects both IPv4 and IPv6 traffic and can be used to monitor most network traffic for data leakage, including HTTP, HTTPS, FTP, FTPS, email, NNTP and instant messaging. DLP also supports the inspection of encrypted traffic.

DLP filters and sensors

DLP filters and sensors are the foundation FortiOS DLP. A filter examines network traffic using one of the different DLP features: document fingerprinting, watermarking, pattern matching, or file filtering. After a filter has been configured, it is then added to a sensor. Sensors combine different filters to meet your specific data leak protection requirements. After a sensor is configured, it is added to a network security policy where it then examines the traffic accepted by that policy.

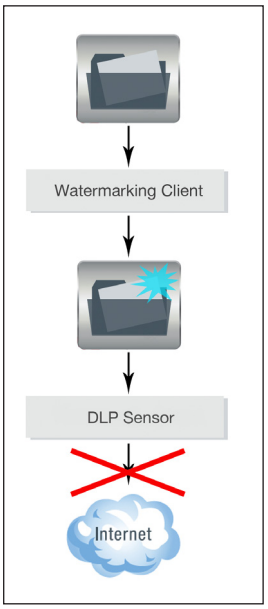
Used together, filters and sensors provide control and flexibility in applying DLP to your security policies, which allows DLP to be used without interfering with the ability of your employees to do their jobs, particularly in situations where work is done either remotely or in collaboration with remote partners.

Document fingerprinting

Every digital file has a unique document fingerprint, also known as a checksum fingerprint. Using FortiOS document printing, you can catalogue the checksum fingerprints of your sensitive documents. Once a fingerprint has been identified, FortiOS is able to track the document even when hidden (for example, when it is inside an archive file).

DLP watermarking

DLP watermarking identifies documents through reading a digital pattern that is added to documents using the Fortinet watermarking client. The process of using watermarks to identify documents is similar to using do cument fingerprinting; however, instead of each document having a unique identifier, a single watermark can be used to identify multiple documents, for example all documents relating to a specific, confidential project. This simplifies the configuration process, as only one DLP filter need s to be configured in order to monitor all files with the specified watermark. Once a watermark has been applied and a DLP filter created, FortiOS can detect watermarked documents and prevent them from being leaked.



Pattern matching

Pattern matching prevents data leaks by examining files and messages for specific patterns within the data's content. FortiOS has two predefined settings for pattern matching: credit card numbers and social security numbers. Regular expressions can also be used to define patterns to be matched. As with the digital markers, when a pattern match is found, the document containing it can be blocked from leaving the network.

File filtering

DLP also provides a range of file filters, which use specific properties to block files from leaving the network. Files can be filtered based on size, name and type (for example, .exe, .pdf, .doc).

DLP archiving

DLP archiving saves a record of all content that matches DLP rules. The records are then sent to a FortiAnalyzer unit and can be used to analyze network traffic and identify potential data leakage risks. Archiving can be done in two ways: summary, which saves a record of the content, or full, which saves all files in the content.

DLP archiving can be used by organizations that require detailed records of the content entering a leaving their network and can be configured to record all content or focus on specific content types.